

NETWORK SERVICES

DATA TRANSFER MODELS

Most services provided by Anchor come with an initial data transfer allocation. Any usage beyond this allocation is charged. Data charging can be based on one of three different models.

If we are charging you based on a data transfer model (options 1 & 2 below) you can transfer data at the full capacity available on our links. We do not shape your traffic in any way. For fixed rates services (option 3) there are no excess data charges although your service may slow if you overload the link.

- 1) Inbound data transfer. We charge you based on the inbound data transfer to your service with outbound being free of charge up to a 1:10 ratio.
- 2) Total data transfer. We charge you for the sum of inbound and outbound data transfer.
- 3) Fixed rate connections. The connection to your service is constrained to the speed of the link you purchase. Within this link you can transfer as much data as the link will sustain.

STANDARD NETWORK CONNECTION

The default connection that is provided with all dedicated server and co-location services is not filtered or firewalled in any way. For these connection types it is important to implement host based firewalling.

SHARED SECURE PORT FIREWALL

A high availability hardware based firewall is configured and managed for your individual server. This service puts you behind a firewall to protect you against unwanted traffic from the Internet. This shared service does not restrict traffic between you and other customers using the same service.

You define the list of ports that you require open and Anchor takes care of the rest. Security advice is provided free of charge in order to assist you define a secure rule set.

PRIVATE SECURE PORT FIREWALL

The private secure port builds on the shared secure port service with addition of VLANs to provide a private firewall service that protects you against other computers on the Internet and all other computers on our network. The

private secure port is much the same as having your own private firewall without absorbing the full running costs.

SECURE SEGMENT FIREWALL

The secure segment is an implementation of the private secure port for customers that have multiple servers on the Anchor network. It provides a cost effective option as the number of servers grows. The secure segment allows unrestricted traffic between servers whilst still protecting it against other servers on our network and the public Internet.

VIRTUAL PRIVATE NETWORK (VPN)

A VPN endpoint is provided to terminate a VPN service between your primary/remote work sites and equipment on the Anchor network using standards based protocols (IPSec & L2TP supported).

Anchor takes care of the complex process of configuring this service and works with you to ensure correct operation of equipment at the remote end of the VPN.

LOAD BALANCING

A network based load balancing service is configured to distribute traffic between two or more servers.

The load balancer is itself a high availability redundant device.

The service can be configured to either share the load between two servers or act in a failover mode to distribute traffic to a primary service until failure is detected.

INTRUSION DETECTION SYSTEM (IDS)

When security is of utmost importance and the risk of attack is very real a managed IDS service can be used to protect your application by detecting malicious traffic before it reaches your server. The service is monitored and customised to your individual requirements.

DATA USAGE REPORTING

All customers can access detailed daily data usage reports on a per IP address basis via an online self service interface.